

PATENT
Atty. Dkt. No. 2000-0415**REMARKS**

In view of the following discussion, the Applicant submits that none of the claims now pending in the application are unpatentable under the provisions of 35 U.S.C. § 103. Thus, the Applicant believes that all of these claims are now in allowable form.

I. REJECTION OF CLAIMS 1-2, 4-6, 8-10, 12-14 AND 16 UNDER 35 U.S.C. § 103

The Examiner has rejected claims 1-2, 4-6, 8-10, 12-14 and 16 in the Final Office Action under 35 U.S.C. § 103 as being unpatentable over Bailey, III (U.S. Patent 5,659,614, issued August 19, 1997, hereinafter referred to as "Bailey") in view of Cane, et al. (U.S. Patent 5,940,507, issued August 17, 1999, hereinafter referred to as "Cane"). The Applicant respectfully traverses the rejection.

Bailey teaches a method and system for creating and storing a backup copy of file data stored on a computer. "The file data to be backed up is encrypted using multiple, indirect encryption keys, variable block lengths, and variable algorithms based on a client-selected string of characters. The files are thereafter encrypted again at the client site prior to transmission to the backup site. A program registry is maintained at the backup site that contains a master copy of many commercially-available files. The incoming files received from the client site are compared to the files in the program registry. If an incoming file is located in the registry, the file is replaced by a token identifying the commercially-available file and the token is stored at the backup facility." (See Bailey, Abstract.)

Cane teaches an information process system that provides archive/backup support with privacy assurance by encrypting relevant stored data. Notably, data generated on a source system is encrypted, the key used thereby is separately encrypted, and both the encrypted data and encrypted key are transmitted to and maintained by a data repository system. (See Cane, Abstract.)

The Examiner's attention is directed to the fact that the combination of Bailey and Cane, alone or in any permissible combination, fails to teach or to suggest the novel concept of deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and generating an authentication code for a bundle that is ultimately added to and encrypted with the bundle, as positively claimed by the

Applicant in claims 1 and 9. In addition, the Applicant submits that the combination of Bailey and Cane fails to teach or to suggest the checking for an authentication code in the compressed bundle, as positively claimed by the Applicant in claims 5 and 13.

Specifically, Applicant's independent claims 1, 5, 9 and 13 positively recite:

1. A method of backing up one or more files on a local device onto remote servers over a network comprising:
deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase;
compressing one or more files and adding each of the files to a bundle;
generating an authentication code for the bundle using the first cryptographic key and adding the authentication code to the bundle; and
encrypting the bundle using the second cryptographic key prior to sending the bundle to the remote server. (Emphasis added.)

5. A method of restoring one or more files on remote servers to a local device over a network comprising:
deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase;
decrypting a bundle received from the remote server using the second cryptographic key;
checking an authentication code in the bundle using the first cryptographic key; and
decompressing one or more files from the bundle. (Emphasis added.)

9. A device-readable medium storing program instructions for performing a method of backing up one or more files on a local device onto remote servers over a network, the method comprising the steps of:
deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase;
compressing one or more files and adding each of the files to a bundle;
generating an authentication code for the bundle using the first cryptographic key and adding the authentication code to the bundle; and
encrypting the bundle using the second cryptographic key prior to sending the bundle to the remote server. (Emphasis added.)

13. A device-readable medium storing program instructions for performing a method of restoring one or more files on remote servers to a local device over a network, the method comprising the steps of:
provided passphrase;
decrypting a bundle received from the remote server using the second cryptographic key;
checking an authentication code in the bundle using the first cryptographic key; and

decompressing one or more files from the bundle. (Emphasis added.)

In one embodiment, the Applicant's invention provides a method and device-readable medium storing program instructions for backing up files from a local device onto remote servers over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and generating an authentication code using the first cryptographic key for a bundle that is ultimately added to and encrypted with the bundle. In addition, Applicant's invention provides a method and device-readable medium storing program instructions for restoring files on remote servers to a local device over a network comprising checking for an authentication code in the compressed bundle.

The Applicant respectfully submits that the combination of Bailey and Cane, alone or in any permissible combination fails to teach or to suggest a method and device-readable medium storing program instructions for backing up files from a local device onto remote servers over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase. Bailey explicitly teaches that "[t]he second encryption is performed by the transmission program based upon internally generated keys." (See Bailey, col. 17, ll. 14-16, emphasis added, see also, Bailey, col. 18, ll. 26-28, "while the second level of encryption is performed by the transmission program that generates its own key," emphasis added.) Moreover, Cane fails to bridge this substantial gap because Cane specifically teaches using a cryptographic engine 14 and key generator 16. (See Cane, col. 3, ll. 51 and 56, FIG. 1.)

Moreover, as indicated by the Examiner on page 3 of the Final Office Action, Bailey fails to disclose the generation of an authentication code for the bundle using the first cryptographic key and adding the authentication code to the bundle. However, the Examiner alleges that Cane teaches this limitation. The Examiner specifically points to Cane, col. 4, ll. 1-27.

The Applicant respectfully submits that the Examiner has interpreted Cane too broadly and must look at Cane in its entirety. The passage cited by the Examiner reads:

"Transmission may be accomplished via Internet 26, dialup connection 28, or in alternative embodiments, other means such as physical delivery of the storage

medium. Encryption may be performed by any of various known methods, such as RSA, DES, and other permutations and may involve authentication and verification either through a trusted third party or mathematical methods. Such authentication and verification may involve cipher block chaining (CBC), to perform an XOR on all or part of a previous block and use the resultant value in encrypting a successive block, or checksums such as cyclic redundancy checks (CRC), MD4, and MD5, which accumulate all values in a particular block according to a mathematical formula to arrive at a value which is highly unlikely to be duplicated if data in the block is changed or lost."

The Applicant respectfully submits that this passage clearly fails to specifically teach generating an authentication code using the first cryptographic key for a bundle that is ultimately added to and encrypted with the bundle, as positively recited in the Applicant's independent claims 1 and 9. The portion of the cited passage mentioning "transmissions" refers to the transmission of encrypted file 20 and encrypted key 24 mentioned earlier in the paragraph and not to the following discussion on encryption. The Applicant respectfully submits that the cited passage in Cane at best generally describes the various methods of encryption and authentication.

Furthermore, Cane clearly teaches away from the Applicant's invention because Cane teaches that a master key is then obtained and used to encrypt the secondary key and produce an encrypted key that is separate from the encrypted file. (See Cane, col. 3, ll. 56-61, emphasis added.) The encrypted file and the encrypted key are then transmitted as separate entities (i.e. not in a single bundle or file) to the archive server as indicated in separate steps 116 and 118. (See Cane, FIG. 2.) Therefore, the Applicant submits that independent claims 1 and 9 fully satisfy the requirements of 35 U.S.C. § 103 and are patentable thereunder.

Finally, both Bailey and Cane completely failed to teach the concept of deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase, as positively claimed by the Applicant. For example, Bailey states that the client key is derived from a client selected string of characters and the actual encryption key is used to encrypt the data are derived from the client key. In other words, the actual encryption key is not generated from the string of characters, but from the client key instead. (See Bailey Column 17, lines 1-5). Similarly, Cane's keys are also not derived from a user-provided passphrase. As such, this element in Applicant's claims is

completely absent in both references. As such, the combination of Bailey with Cane simply cannot make Applicant's independent claims obvious.

Applicant also respectfully submits that the combination of Bailey and Cane, alone or in any permissible combination fails to teach or to suggest a method and device-readable medium storing program instructions for restoring files on remote servers to a local device over a network comprising checking for an authentication code in the compressed bundle, as positively recited in the Applicant's independent claims 5 and 13. As indicated on page 4 of the Final Office Action by the Examiner, Bailey does not expressly disclose the checking of an authentication code in the bundle using the first cryptographic key. However, the Examiner alleges that Cane teaches this limitation.

In response, the Applicant respectfully submits that Bailey and Cane do not disclose, mention or suggest the checking of an authentication code in a bundle using the first cryptographic key. More specifically, the Applicant contends that Cane only teaches an archive server that first writes the encrypted file to a medium and subsequently writes the encrypted key to another medium separately. Notably, the Applicant submits that Cane does not teach a checking process of any type. Therefore, the Applicant contends that since a bundle comprising an authentication code along with a plurality of files is not taught by Cane, it is impossible for the bundle to be checked (i.e., since a bundle does not exist.)

In fact, Cane teaches away from the Applicant's invention because the recovery process taught by Cane specifically teaches that first the secondary key must be recovered by decrypting the encrypted key with the master key, which is located separately on cryptographic engine 14. (See Cane, col. 4, ll. 27-37, FIG 1.) Then the original file is recovered by decrypting the encrypted file with the secondary key, which is also located separately. (See *Id.*) Consequently, the Applicant respectfully submits that independent claims 5 and 13 fully satisfy the requirements of 35 U.S.C. § 103 and are patentable thereunder.

In addition, dependent claims 2, 4, 6, 8, 10, 12, 14 and 16 depend, either directly or indirectly, from independent claims 1, 5, 9 and 13 and recite additional limitations. As such, and for the exact same reason set forth above, the Applicant submits that claims

PATENT
Atty. Dkt. No. 2000-0415

2, 4, 6, 8, 10, 12, 14 and 16 also fully satisfy the requirements of 35 U.S.C. § 103. As such, Applicant respectfully requests the rejection be withdrawn.

II. REJECTION OF CLAIMS 3, 7, 11 AND 15 UNDER 35 U.S.C. § 103

The Examiner has rejected claims 3, 7, 11 and 15 in the Final Office Action under 35 U.S.C. § 103 as being unpatentable over Bailey in view Cane in further view of Walmsley (US Publication 2004/0049468, published March 11, 2004, hereinafter referred to as "Walmsley"). The Applicant respectfully traverses the rejection.

The teachings of Bailey and Cane have been discussed above. Walmsley teaches "a consumable authentication method for validating the existence of an untrusted chip. A random number is encrypted using a first key and sent to an untrusted chip. In the untrusted chip it is decrypted using a secret key and re-encrypted together with a data message read from the untrusted chip. This is decrypted so that a comparison can be with the generated random number and the read data message." (See Walmsley, Abstract.)

The Applicant respectfully submits that Walmsley does not bridge the substantial gap existing between the Applicant's invention and the combination of Bailey and Cane. More specifically, the Applicant contends that Walmsley does not teach, show or suggest deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and generating an authentication code for a bundle that is ultimately added to and encrypted with the bundle as set forth in claims 1, 5, 9 and 13. The Examiner's attention is directed to the fact that Bailey in view of Cane in further view of Walmsley fails to disclose or suggest the novel concept of deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and generating an authentication code for a bundle that is ultimately added to and encrypted with the bundle as claimed in Applicant's independent claims 1 and 9, from which claims 3 and 11 depend. Similarly, Bailey in view of Cane in further view of Walmsley fails to disclose or suggest the novel concept of deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and checking for an authentication code that was encrypted in the bundle using a first cryptographic key

PATENT
Atty. Dkt. No. 2000-0415

as claimed in Applicant's independent claims 5 and 13, from which claims 7 and 15 depend.

Consequently, the Applicant submits that claims 1, 5, 9 and 13 would not be made obvious by the teaching of Bailey in view of Cane in further view of Walmsley, and therefore, are patentable under 35 U.S.C. § 103.

Since claims 3, 7, 11 and 15 depend, either directly or indirectly, from claims 1, 5, 9 and 13, and recite additional limitations, the Applicant submits that claims 3, 7, 11 and 15 are also not made obvious by the teaching of Bailey in view of Cane in further view of Walmsley. Therefore, the Applicant submits that claims 3, 7, 11 and 15 also fully satisfy the requirements of 35 U.S.C. § 103 and are patentable thereunder. As such, the Applicant respectfully request the rejection be withdrawn.

CONCLUSION

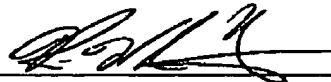
Thus, the Applicant submits that all of these claims now fully satisfy the requirements of 35 U.S.C. § 103. Consequently, the Applicant believes that all these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring the maintenance of the present final action in any of the claims now pending in the application, it is requested that the Examiner telephone Mr. Kin-Wah Tong, Esq. at (732) 530-9404 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully Submitted,

January 18, 2006

Patterson & Sheridan, LLP
595 Shrewsbury Avenue
Shrewsbury, New Jersey 07702



Kin-Wah Tong, Attorney
Reg. No. 39,400
(732) 530-9404